UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

VICTOR JAMES COMFORTE, II and BRENDAN MICHAEL CARR, individually, and on behalf of all others similarly situated, Plaintiffs, v. CAMBRIDGE ANALYTICA, FACEBOOK, INC., MARK ZUCKERBERG, and JOHN and JANE DOES 1-100, Defendants.	**JURY DEMANDED** CASE No. 1:18-cv-02120

CLASS ACTION COMPLAINT

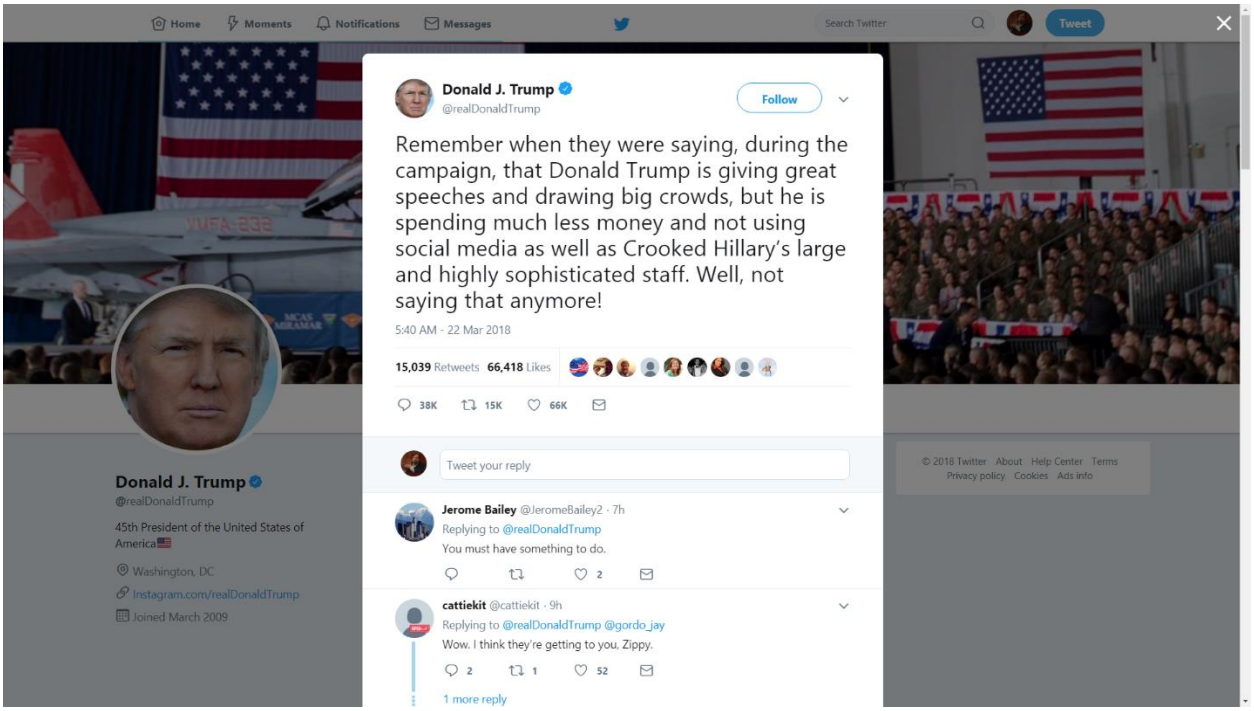
Plaintiffs VICTOR JAMES COMFORTE, II and BRENDAN MICHAEL CARR ("Plaintiff"), individually, and on behalf of all others similarly situated, by and through their attorney James C. Vlahakis of SULAIMAN LAW GROUP, LTD., assert A Class Action Complaint against Defendants CAMBRIDGE ANALYTICA, LLC, FACEBOOK, INC., MARK ZUCKERBERG, and JOHN and JANE DOES 1-100, pursuant to the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510 et seq., the Stored Communications Act, 18 U.S.C. §§ 2701, et seq., the Illinois Consumer Fraud and Deceptive Practices Act and other common law causes of action:

INTRODUCTION

1. CAMBRIDGE ANALYTICA, LLC ("Cambridge") is privately held company that has been actively engaged in data mining, data brokerage, and data analysis with for the purpose of influencing the electoral process. As detailed below, Cambridge used the personal information of millions of Facebook users to influence the 2016 United States presidential election.

2. Will Bunch of *The Inquirer* questioned whether the winner of the 2016 presidential election admitted to this scheme in a tweet at 5:44 a.m. on March 22, 2018:

> Bizarrely, Trump himself seemed to acknowledge in a tweet this Thursday morning that the messages crafted by CA were critical to his victory.



Mr. Bunch's article is at http://www.philly.com/philly/columnists/will_bunch/race-realism-steve-bannon-cambridge-analytica-elected-trump-20180322.html

PARTIES, JURISDICTION AND VENUE

3. Cambridge was created in 2013 as an offshoot of its British parent company SCL Group to participate in American politics.

4. In 2014, Cambridge was reportedly involved in 44 political races in the United States.

5. Cambridge has offices in London, New York City and Washington, D.C., among other U.S. cities.

6. Cambridge's C.E.O., Alexander Nix ("Nix"), has admitted to using tricks to influence elections. *See*, http://www.theweek.co.uk/92390/cambridge-analytica-ceo-admits-to-dirty-tricks.

7. FACEBOOK INC. ("Facebook") is a publically traded company, incorporated in Delaware, and is headquartered in Menlo Park, California 94025.

8. Mark Zuckerberg is the C.E.O. of Facebook and a resident of California.

9. Zuckerberg has continuously conducted business for Facebook in the City of Chicago and has done so as recently as June of 2017. See, https://www.facebook.com/zuck/posts/10103819315413091

10. Plaintiff VICTOR JAMES COMFORTE, II ("Comforte") is a registered voter residing in the Northern District of Illinois.

11. Plaintiff BRENDAN MICHAEL CARR ("Carr") is a registered voter residing in the Northern District of Illinois.

12. Pursuant to 28 U.S.C. § 1331, this Court has original subject matter jurisdiction over the claims of Plaintiffs and the Class that arise under the Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. §§ 2510 et seq.

13. The ECPA provides that any person whose electronic communication is "intercepted, disclosed, or intentionally used" in violation of the Act may in a civil action recover from the entity which engaged in that violation. 18 U.S.C. § 2520(a).

14. Title I of ECPA is commonly referred to as the Wiretap Act and Tittle II of ECPA is commonly referred to as the Stored Communications Act.

15. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than

100 class members, and at least one class member is a citizen of a state different from Defendants and is a citizen of a foreign state.

16. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

17. Venue is proper under 28 U.S.C. § 1391(c) because Defendants are corporations that do business in and are subject to personal jurisdiction in this District.

18. Venue is also proper because a substantial part of the misconduct and deception giving rise to the claims in this action took place this District.

SUMMARY OF ALLEGATIONS RELATED TO DEFENDANTS' MISCONDUCT

19. This civil action is about a severe and unprecedented *breach of trust* committed by the Defendants which allowed Cambridge, to secretly and unlawfully mine the sensitive personal data of at least 300,000 Facebook users to help Cambridge and its cronies manipulate and misuse Facebook to target voters to help influence the results of the 2016 Presidential Election.

20. Facebook has over 2 billion users.

21. Plaintiffs Comforte and Carr are Facebook users and were Facebook users at all times during the events discussed herein.

22. Facebook's "Data Use Policy" emphasizes "trust" and states that "we don't share information we receive about you with others unless we have . . . received your permission [and] given you notice."

23. As detailed below, in contrast to policies and statements attributable to Defendants Zuckerberg, during the 2016 Presidential election, while using Facebook to communicate with friends, review posts from friends and read stories posted by friends and others on Facebook, Plaintiffs and other Facebook were targeted with political ads and posts.

24. Plaintiffs and other Facebook users were targeted with political ads and posts were generated as part of a data mining scheme involving Cambridge and various John and Jane Doe Defendants.

25. According to *The Washington Post* has reported that Steve Bannon, a former "chief political strategist" to the current sitting President[i] of the United States, "oversaw Cambridge Analytica's early efforts to collect troves of Facebook data as part of an ambitious program to build detailed profiles of millions of American voters[.]" According to the Post, "[m]ore than three years before he served as Trump's chief political strategist, Bannon helped launch Cambridge Analytica with the financial backing of the wealthy Mercer family as part of a broader effort to create a populist power base."[1]

26. In March 2018, *The Guardian* reported that Nix talked "unguardedly about the company's practices" when he was secretly filmed by British television reporters posing as prospective clients and that Cambridge was trying to stop the resulting footage.[2]

27. The secret filming was screened on 19 March as part of a 30-minute segment, with a follow-up scheduled for the next day, focusing on Cambridge's involvement in the campaign for the current President of the United States. The conversation appears to portray Nix including entrapment and bribery as potential CAMBRIDGE services. *See,* https://www.nytimes.com/2018/03/19/us/cambridge-analytica-alexander-nix.html

[1] https://www.washingtonpost.com/politics/bannon-oversaw-cambridge-analyticas-collection-of-facebook-data-according-to-former-employee/2018/03/20/8fb369a6-2c55-11e8-b0b0-f706877db618_story.html?utm_term=.bb64b923e5e1

[2] https://www.theguardian.com/news/2018/mar/18/cambridge-analytica-and-facebook-accused-of-misleading-mps-over-data-breach.

28. In contrast to recent disclosures from Defendant Zuckerberg, in February 2018, Nix told the British Parliament's Digital, Culture, Media and Sport Committee ("DCMSC") that Cambridge had not received any data from Facebook.

29. *The Guardian* has reported that Damain Collins, the DCMSC's committee chair, recalled Nix to testify a second time, stating, among other things:

> "Following material published in the UK Guardian, the New York Times and Channel 4 over the past few days, the committee would like to request that you supply further evidence[.]"
>
> "There are a number of inconsistencies in your evidence to us, notably your denial that your company received data from the Global Science Research company. We are also interested in asking you again about your claim that you 'do not work with Facebook data, and … do not have Facebook data'."

See, https://www.theguardian.com/uk-news/2018/mar/22/cambridge-analytica-warrant-high-court-adjourns-hearing-information-commissioner

30. On 20 March 2018, Nix was reportedly suspended from Cambridge. *See,* http://www.bbc.co.uk/news/uk-43480048

31. Just recently, it was disclosed by *The Guardian* that Cambridge, on its own, and/or in conjunction with Facebook, and one or more of the John Doe Defendants, helped influence the 2016 United States presidential election by (a) obtaining the personal information of thousands of Facebook users under false pretenses, (b) mining and manipulating users' personal information, (c) and targeting voters with the inappropriately obtained information (d) for the sole purpose of stealing the election for the current sitting President of the United States.

32. Cambridge undertook this scheme through its manipulation of a thir-party app called *MyDigitalLife*.

33. In an interview in *The Guardian*, Christopher Wylie, a former contractor for Cambridge explained how the data mining worked: "With their profiles, likes, even

private messages, [Cambridge] could build a personality profile on each person and know how best to target them with messages."

34. Wylie told *The Guardian* that he has documents that demonstrate "how, between June and August 2014, the profiles of more than 50 million Facebook users had been harvested."

35. Wylie told *The New York Times* that he had access to the Facebook profiles which "contained enough information, including places of residence, that [Cambridge] could match users to other records and build psychographic profiles."

36. Wylie told *The New York Times* that Cambridge's access to "the Facebook data…was 'the saving grace' that let his team deliver the models it had promised the Mercers."

37. The Mercer family, reportedly adhere to and promote far-right/conservative political positions.[3]

38. On information and belief, the Mercer family sought to mine Facebook profiles to help win the 2016 Presidential Election for the current sitting President.

39. *The Guardian* published detailed expose on Cambridge's data mining and meddling with the 2016 Presidential election, which can be found at https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

40. In this article, *Wylie* told *The Guardian* that he helped create "Steve Bannon's psychological warfare mindfuck tool."

41. According to *The Guardian*, Cambridge used MyDigitalLife to obtain the personal information of approximately 300,000 Facebook users and mined the data it obtained from these persons to obtain access to their friends' data.

[3] Plaintiffs will amend this action to name additional defendants as their investigation continues.

42. Ultimately, Cambridge scheme allowed it to use *MyDigitalLife* to obtain the personal information of 50 million other persons.

43. Sasha Issenberg, an experienced writer in the field of "data in politics" described what Cambridge does – and how it differs from other data analysis firms:

> In my years of writing about the use of data in politics, other firms had developed a variety of profiles of me using public and private sources; each time I was told what campaigners who had never interacted with me assumed about my identity or attitudes. I had seen statistical models anticipating my likelihood of casting a ballot in various upcoming elections, of being married, of owning a gun. In an ideal world, campaigns would have access to this information from a less speculative source: my telling a canvasser how I intended to vote, a warranty form on which I had identified a spouse, or the inclusion of my name on a publicly available list of licensed hunters or private membership rolls shared by the National Rifle Association. But if those were not available, or out of date, statistical models could make inferences from facts that were available. Algorithms could trawl through as many of thousands of different variables—my past political behavior, consumer choices, the demographic composition of the Philadelphia neighborhood in which I was registered—and isolate the interaction of a few that would determine how much I statistically resembled people who were known to be married, or to own a gun. Campaigns could then communicate with me based on those calculated likelihoods.
>
> Cambridge Analytica's assessment differed in one crucial way: The firm promised to tell me things I might not even know about myself. It claimed to predict where I would fall on the five-factor personality model, which won widespread adoption by psychologists starting in the 1980s as a standard inventory of universal traits known as "the Big Five." According to Cambridge Analytica, I fell in the middle range for extroversion. When it came to neuroticism, I was in the seventieth percentile. I scored very low on conscientiousness and agreeableness, a combination which, when paired with my high openness, defined my individualism. "Fanciful/Imaginative Types are unconventional nonconformists who pride themselves on being different from others," read a potted description attached to my numerical assessment. "In extreme cases they might be regarded as eccentric, but in most cases they are perceived by others as complex, well-read, imaginative and industrious."
>
> Of all the microtargeting profiles of myself I had seen, none had flattered my self-concept like this one. Its predictions already seemed more plausible than those of the Democratic data warehouse that had my religion pegged as Lutheran—a prediction likely tethered to the only slightly less dubious profiling of my ethnicity as German. (I presume that was the result of an algorithm which heavily weighted my surname's

> Teutonic build and the preponderance of white people in my census tract who report German ancestry.)
>
> "And so you can imagine with that information as well as all the other information about your political orientation it is possible to put you with the like-minded people to receive a very, very specific communication," Cambridge CEO Alexander Nix told me.
>
> * * *
>
> After the 2012 election, Nix found an American marketplace far more receptive to his entreaties. The overseas work in conflict zones amounted to a promising calling card, a new comparative advantage over entrenched American political firms. "This is really trying to use psychology to understand why hostile audiences do what they do, and to use this methodology to deconstruct that behavior and then use communication to try and change attitudes and ultimately behavior," Nix says. "Persuading somebody to vote in a certain way," he goes on, "is really very similar to persuading 14- to 25-year-old boys in Indonesia to not join Al Qaeda."

See, https://www.bloomberg.com/news/features/2015-11-12/is-the-republican-party-s-killer-data-app-for-real-

44. Issenberg's article discussed how Cambridge utilized its purported access to Facebook profiles to measure "likely attributes":

> A decade ago, the centre's David J. Stilwell and Michal Kosinski uncovered a new way to get people to part with personal data: social-media quizzes. Since their MyPersonality app was launched in 2007, six million people have completed the questionnaire—nearly half of them allowing the Cambridge's Psychometrics Centre to access their Facebook profiles as they did so. Once a user grants such access, algorithms trawl through likes and posts to train statistical models that use such "digital footprints" to predict personality types. Scholars are allowed to dip into that pool of anonymized data for worthy academic research, and the fruits of those models are promoted commercially as Apply Magic Sauce, a data stream that allows online marketers to adjust their appeals to potential consumers based on their likely attributes.
>
> * * *
>
> A few weeks after I visited their London office, I went to the University of Cambridge Psychometrics Centre's website to see what I could learn about myself from a psychological assessment detached from political considerations. The centre's site shows users who sign in with their Facebook accounts the personality profile that Apply Magic Sauce generates from their digital footprints, but I hadn't liked or posted enough to adequately feed its algorithm[.]

Id.

TIMELINE OF EVENTS AS DESCRIBED BY DEFENDANT ZUCKERBERG

45. In 2007, Defendants Zuckerberg and Facebook "launched the Facebook Platform with the vision that more apps should be social."

46. Zuckerberg, as Facebook's CEO, is a well-known public figure, who take a hands on approach to managing Facebook's privacy and policies.

47. On March 21, 2018, Defendant Zuckerberg, posted an explanation of Cambridge's misconduct which explained that "[Facebook] enabled people to log into apps and share who their friends were and some information about them." See, https://www.facebook.com/zuck/posts/10104712037900071

48. "In 2013, a Cambridge University researcher named Aleksandr Kogan created a personality quiz app." *Id.*

49. The Guardian has described Kogan as follows:

> Aleksandr Kogan was born in Moldova and lived in Moscow until the age of seven, then moved with his family to the US, where he became a naturalised citizen. He studied at the University of California, Berkeley, and got his PhD at the University of Hong Kong before joining Cambridge as a lecturer in psychology and expert in social media psychometrics. He set up Global Science Research (GSR) to carry out CA's data research. While at Cambridge he accepted a position at St Petersburg State University, and also took Russian government grants for research. He changed his name to Spectre when he married, but later reverted to Kogan.

See, https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

50. Zuckerberg's post claims that Kogan's app "was installed by around 300,000 people who shared their data as well as some of their friends' data." *Id.*

51. Zuckerberg's post did not identify how many of the 300,000 people shared their friends' data.

52. Given the way [Facebook's] platform worked at the time this meant Kogan was able to access tens of millions of their friends' data." *Id.*

53. Defendant Zuckerberg went on to state:

> "In 2014, to prevent abusive apps, we announced that we were changing the entire platform to dramatically limit the data apps could access. Most importantly, apps like Kogan's could no longer ask for data about a person's friends unless their friends had also authorized the app. We also required developers to get approval from us before they could request any sensitive data from people. These actions would prevent any app like Kogan's from being able to access so much data today."

54. Defendant Zuckerberg's March 21, 2018 Facebook post does not indicate whether or Facebook conducted any investigations to determine whether third-party apps had improperly obtained access to users' personal information without obtained users' permission.

55. On information and belief, Defendant Zuckerberg did not conduct any investigations to determine whether third-party apps had improperly obtained access to users' personal information without obtained users' permission.

56. On information and belief, Facebook did not conduct any investigations to determine whether third-party apps had improperly obtained access to users' personal information without obtained users' permission.

57. It appears that Defendant Zuckerberg and Facebook did not conduct any investigations because if they had, they were have learned on their own about the misconduct of Cambridge rather than learning about it from a reporter from *The Guardian*, *The New York Times* and British television, Chanel 4.

58. According to Zuckerberg's March 21, 2018 Facebook post:

> "In 2015, we learned from journalists at The Guardian that Kogan had shared data from his app with Cambridge Analytica. It is against our policies for developers to share data without people's consent, so we immediately banned Kogan's app from our platform, and demanded that Kogan and Cambridge Analytica formally certify

> that they had deleted all improperly acquired data. They provided these certifications."

59. Zuckerberg, Facebook and other John Doe Defendants did not undertake reasonable measures to ensure that Cambridge deleted the personal information of FACEBOOK users that was improperly obtained by Cambridge.

60. We know this to be the case because Defendant Zuckerberg's March 21, 2018 Facebook post conceded that Cambridge *did not delete* the improperly obtained personal information of Facebook users.

61. According to Zuckerberg's March 21, 2018 Facebook post:

> Last week, we learned from The Guardian, The New York Times and Channel 4 that Cambridge Analytica may not have deleted the data as they had certified. We immediately banned them from using any of our services. Cambridge Analytica claims they have already deleted the data and has agreed to a forensic audit by a firm we hired to confirm this. We're also working with regulators as they investigate what happened.

62. Zuckerberg's March 21, 2018 Facebook post apologized for Zuckerberg and Facebook's inaction, calling it a "breach of trust between Facebook and the people who share their data with us and expect us to protect it".

63. Defendant Zuckerberg's full quote on this issue is listed below.

> This was a breach of trust between Kogan, Cambridge Analytica and Facebook. But it was also a breach of trust between Facebook and the people who share their data with us and expect us to protect it. We need to fix that.

64. While Defendant Zuckerberg's March 21, 2018 Facebook post implied that Facebook had investigated Cambridge's misconduct in 2013, it is clear that Defendant Zuckerberg, Facebook and other John Doe Defendants *did not undertake reasonable measures* to "prevent bad actors from accessing people's information in this way."

65. In part, Defendant Zuckerberg's March 21, 2018 Facebook post suggests that Facebook is only now conducting a "full audit." According to Defendant Zuckerberg's March 21, 2018 Facebook post:

> We will conduct a full audit of any app with suspicious activity. We will ban any developer from our platform that does not agree to a thorough audit. And if we find developers that misused personally identifiable information, we will ban them and tell everyone affected by those apps. That includes people whose data Kogan misused here as well.

66. Notably, Zuckerberg's March 21, 2018 Facebook post does not indicate that he, or Facebook, took any effort to notify Facebook users, in 2013, 2014, 2015, 2016 or 2017 that Cambridge had "misused personally identifiable information."

67. Rather, only after *The Guardian*, *The New York Times* and Chanel 4 published the news did Defendant Zuckerberg or Facebook make any public statement to Facebook users.

68. Facebook executives have tweeted that Facebook users were not subjected to a "data breach" as the term has been reported in the press.

69. Alex Stamos, Facebook's Chief Security Officer, tweeted the following:

Alex Stamos
@alexstamos

The recent Cambridge Analytica stories by the NY Times and The Guardian are important and powerful, but it is incorrect to call this a "breach" under any reasonable definition of the term. We can condemn this behavior while being accurate in our description of it.

3/17/18, 12:20 PM

27 Retweets **53** Likes

70. Stamos subsequently deleted this tweet.

71. In fairness, the complete text of Zuckerberg March 21, 2018, post is pasted below:

> I want to share an update on the Cambridge Analytica situation -- including the steps we've already taken and our next steps to address this important issue.

We have a responsibility to protect your data, and if we can't then we don't deserve to serve you. I've been working to understand exactly what happened and how to make sure this doesn't happen again. The good news is that the most important actions to prevent this from happening again today we have already taken years ago. But we also made mistakes, there's more to do, and we need to step up and do it.

Here's a timeline of the events:

In 2007, we launched the Facebook Platform with the vision that more apps should be social. Your calendar should be able to show your friends' birthdays, your maps should show where your friends live, and your address book should show their pictures. To do this, we enabled people to log into apps and share who their friends were and some information about them.

In 2013, a Cambridge University researcher named Aleksandr Kogan created a personality quiz app. It was installed by around 300,000 people who shared their data as well as some of their friends' data. Given the way our platform worked at the time this meant Kogan was able to access tens of millions of their friends' data.

In 2014, to prevent abusive apps, we announced that we were changing the entire platform to dramatically limit the data apps could access. Most importantly, apps like Kogan's could no longer ask for data about a person's friends unless their friends had also authorized the app. We also required developers to get approval from us before they could request any sensitive data from people. These actions would prevent any app like Kogan's from being able to access so much data today.

In 2015, we learned from journalists at The Guardian that Kogan had shared data from his app with Cambridge Analytica. It is against our policies for developers to share data without people's consent, so we immediately banned Kogan's app from our platform, and demanded that Kogan and Cambridge Analytica formally certify that they had deleted all improperly acquired data. They provided these certifications.

Last week, we learned from The Guardian, The New York Times and Channel 4 that Cambridge Analytica may not have deleted the data as they had certified. We immediately banned them from using any of our services. Cambridge Analytica claims they have already deleted the data and has agreed to a forensic audit by a firm we hired to confirm this. We're also working with regulators as they investigate what happened.

This was a breach of trust between Kogan, Cambridge Analytica and Facebook. But it was also a breach of trust between Facebook and the people who share their data with us and expect us to protect it. We need to fix that.

> In this case, we already took the most important steps a few years ago in 2014 to prevent bad actors from accessing people's information in this way. But there's more we need to do and I'll outline those steps here:
>
> First, we will investigate all apps that had access to large amounts of information before we changed our platform to dramatically reduce data access in 2014, and we will conduct a full audit of any app with suspicious activity. We will ban any developer from our platform that does not agree to a thorough audit. And if we find developers that misused personally identifiable information, we will ban them and tell everyone affected by those apps. That includes people whose data Kogan misused here as well.
>
> Second, we will restrict developers' data access even further to prevent other kinds of abuse. For example, we will remove developers' access to your data if you haven't used their app in 3 months. We will reduce the data you give an app when you sign in -- to only your name, profile photo, and email address. We'll require developers to not only get approval but also sign a contract in order to ask anyone for access to their posts or other private data. And we'll have more changes to share in the next few days.
>
> Third, we want to make sure you understand which apps you've allowed to access your data. In the next month, we will show everyone a tool at the top of your News Feed with the apps you've used and an easy way to revoke those apps' permissions to your data. We already have a tool to do this in your privacy settings, and now we will put this tool at the top of your News Feed to make sure everyone sees it.
>
> Beyond the steps we had already taken in 2014, I believe these are the next steps we must take to continue to secure our platform.
>
> I started Facebook, and at the end of the day I'm responsible for what happens on our platform. I'm serious about doing what it takes to protect our community. While this specific issue involving Cambridge Analytica should no longer happen with new apps today, that doesn't change what happened in the past. We will learn from this experience to secure our platform further and make our community safer for everyone going forward.
>
> I want to thank all of you who continue to believe in our mission and work to build this community together. I know it takes longer to fix all these issues than we'd like, but I promise you we'll work through this and build a better service over the long term.

FACEBOOK WAS WARNED OF THE RISK OF IMPROPER DATA MINING

72. As discussed below, Defendants Zuckerberg and Facebook knew of Cambridge's improper data mining and misuse of the personal information of hundreds

of thousands of Facebook users, but Zuckerberg and Facebook (and other currently unknown John and Jane Doe Defendants) ignored Cambridge's misconduct.

73. Zuckerberg and Facebook acted this way despite the fact that Facebook is subject to a consent decree with the Federal Trade Commission relative to the interplay of "privacy settings" where the consent decree was intended to prevent Facebook users from being "forced to share more Personal information than [users] intended."

74. Defendants' collective misconduct caused Plaintiffs' Facebook news feeds to be flooded with unwanted political messages – all in a misguided effort to sway them to vote for the current President of the United States.

75. Defendants' collective misconduct caused Plaintiffs' Facebook news feeds to be bombarded by disruptive and contentious political messages and advertisements – including political messages and advertisements that Plaintiffs did not agree with.

76. A Facebook user named Max Schrems forewarned Facebook of the potential mining and misuse of user data in as early as August of 2011 when he filed a Complaint against "Facebook Ireland Ltd." ("Facebook Ireland") with the Irish based Office of the Data Protection Commissioner ("ODPC").

77. Facebook Ireland, is Defendant Facebook's Irish subsidiary and the location of its European headquarters.

78. On information and belief, Schrems is a German privacy rights lawyer.

79. A copy of Mr. Schrems' Complaint is posted at http://www.europe-v-facebook.org/Complaint_13_Applications.pdf

80. A "Media Update" issued by *noyb* highlights how Schrems warned Facebook Ireland of the risk of data mining by a nefarious third-party.

81. According to *noyb's* "Media Update":

> Max Schrems (chairman of noyb.eu) is surprised by Facebook's reaction on the Cambridge Analytica scandal: *"Facebook has millions of times*

illegally distributed data of its users to various dodgy apps - without the consent of those affected. In 2011 we sent a legal complaint to the Irish Data Protection Commissioner on this. Facebook argued that this data transfer is perfectly legal and no changes were made. Now after the outrage surrounding Cambridge Analytica the Internet giant suddenly feels betrayed seven years later. Our records show: Facebook knew about this betrayal for years and previously argues that these practices are perfectly legal."

82. The "Media Update" is posted at https://noyb.eu/wp-content/uploads/2018/03/Media-Update-Cambridge-Analytica-en.pdf

83. In relevant part, Mr. Schrems' Complaint reads as follows:

Facebook Ireland offers all its users the option to use third party "applications" on facebook.com. These applications are developed, managed and run by third party companies that can be situated anywhere in the world. The applications run on external systems but Facebook Ireland allows the providers of the applications access to the data it is hosting. According to Facebook Ireland's statistics page there are more than 20 million applications installed by users every day.

This constitutes a tremendous threat to data privacy on facebook.com. There are only very limited contractual measures that Facebook Ireland is taking to ensure that developers of applications have an adequate level of data protection (see the yellow text in attachment 03).

There is no way that Facebook Ireland would be able to ensure real compliance with these limited contractual measures. The Wall Street Journal found out in October 2010 that "all of the 10 most popular apps on Facebook were transmitting users' IDs to outside companies" (see attachment 04). Another example: Many applications do not even have a privacy policy, even though Facebook Ireland requires this. When I was checking on the 12 applications Facebook was randomly suggesting on my profile, 4 did not have a policy while 5 did have a policy right after I clicked on them (see attachment 05). Apparently Facebook Ireland is not even enforcing this very basic provision.

When the user connects to an application that does not have a privacy policy, facebook.com simply hides the link that would usually bring you to the privacy policy, instead of warning the user that there is not even a privacy policy (see e.g. page 5 of attachment 05). While Facebook USA is a member of the Safe Harbor Agreement, developers are not obliged to be a member of Safe Harbor. This means that Facebook Ireland is exporting personal data to other companies that do not have an adequate level of data protection, including companies in the USA which are not member of the Safe Harbor.

Most users are not aware that if a "friend" on facebook.com installs an application, the application can automatically access their profile picture, name and other basic information (see privacy policy in attachment 06). Note that

> Facebook Ireland is hiding this consent for the use of other users' data under the section "my basic information" (see e.g. page 4 in attachment 05)
>
> If the person that is installing the application is consenting to it, the application can read all information about all friends that the person can see. Again this means that not the data subject but "friends" of the data subject are consenting to the use of personal data. Since an average facebook user has 130 friends, it is very likely that only one of the user's friends is installing some kind of spam or phishing application and is consenting to the use of all data of the data subject. There are many applications that do not need to access the users' friends personal data (e.g. games, quizzes, apps that only post things on the user's page) but Facebook Ireland does not offer a more limited level of access than "all the basic information of all friends".
>
> All this can only be prevented if the user turns off "platform" (opt-out). This can be done by clicking a button which is again well hidden (see attachment 07). There is no possibility to use applications without the possibility that other users can access the user's data (all or nothing). The data subject is not given an unambiguous consent to the processing of personal data by applications (no opt-in).
>
> Even if a data subject is aware of this entire process, the data subject cannot foresee which application of which developer will be using which personal data in the future. Any form of consent can therefore never be specific.
>
> Facebook Ireland could not answer me which applications have accessed my personal data and which of my friends have allowed them to do so. Therefore there is practically no way how I could ever find out if a developer of an application has misused data it got from Facebook Ireland in some way.

http://www.europe-v-facebook.org/Complaint_13_Applications.pdf at pp. 2-3.

84. As a result of Mr. Schrems' Complaint, the ODPC investigated the Complaint and issued a "Report of Re-Audit" ("Report") on September 21, 2012.

85. Katherrine Tassi, Facebook's former head of data protection, was involved with Facebook's response to ODPC's investigation, having authored Facebook Ireland's response to the investigation. Facebook Ireland is Facebook's European division.

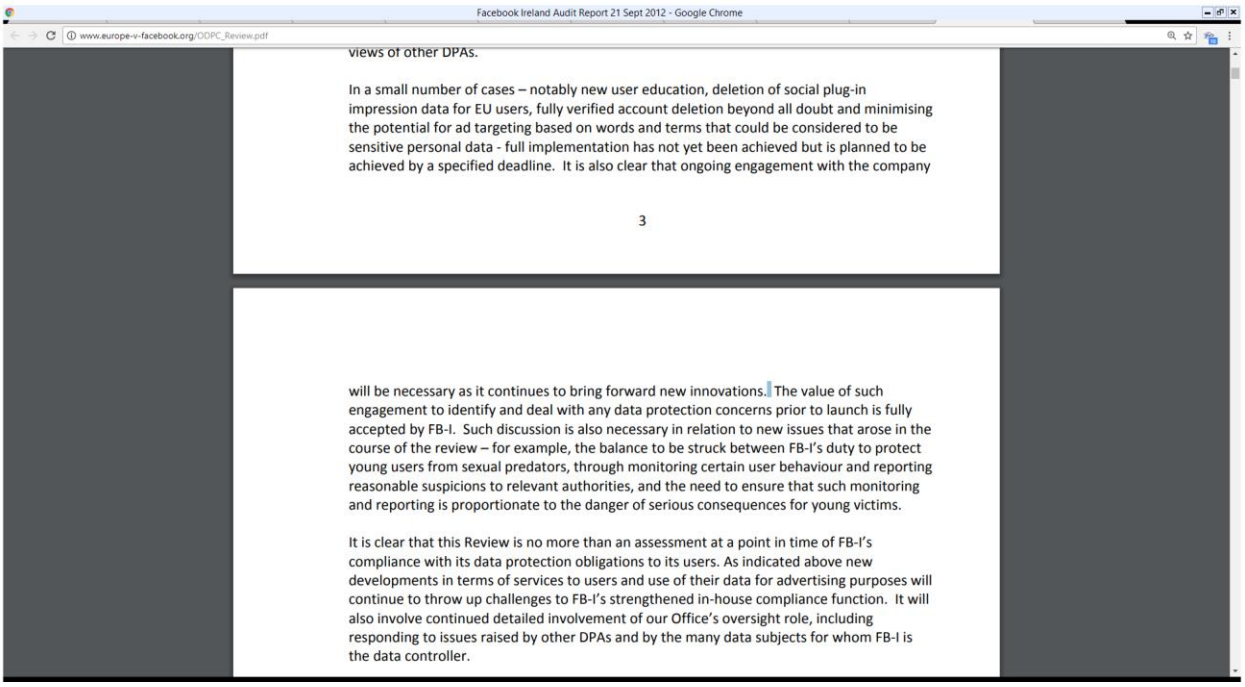
86. Tassi spent 4 years at Facebook as the Head of Data Protection and the Associate General Counsel in charge of the global data protection program.

87. Prior to working at Facebook, Tassi spent 8 years serving in the Washington State Attorney General's Office as an Assistant Attorney General prosecuting consumer protection violations and working on high-tech litigation.

88. While at Uber, Ms. Tassi wrote a reported and amended her reporting of a 2014 data breach at Uber. *See,* https://www.uber.com/newsroom/uber-statement/

89. Ironically (perhaps), Uber hired Facebook's former chief security office, Joe Sullivan, who was subsequently fired by Uber in 2017 for hiding a 2016 data breach involving the personal information of 57 million Uber riders and drivers.

90. ODPC's Report stated that Facebook Ireland had yet to adopt complete protection of "sensitive personal data." According to the Report:


Facebook Ireland Audit Report 21 Sept 2012 - Google Chrome

www.europe-v-facebook.org/ODPC_Review.pdf

views of other DPAs.

In a small number of cases – notably new user education, deletion of social plug-in impression data for EU users, fully verified account deletion beyond all doubt and minimising the potential for ad targeting based on words and terms that could be considered to be sensitive personal data - full implementation has not yet been achieved but is planned to be achieved by a specified deadline. It is also clear that ongoing engagement with the company

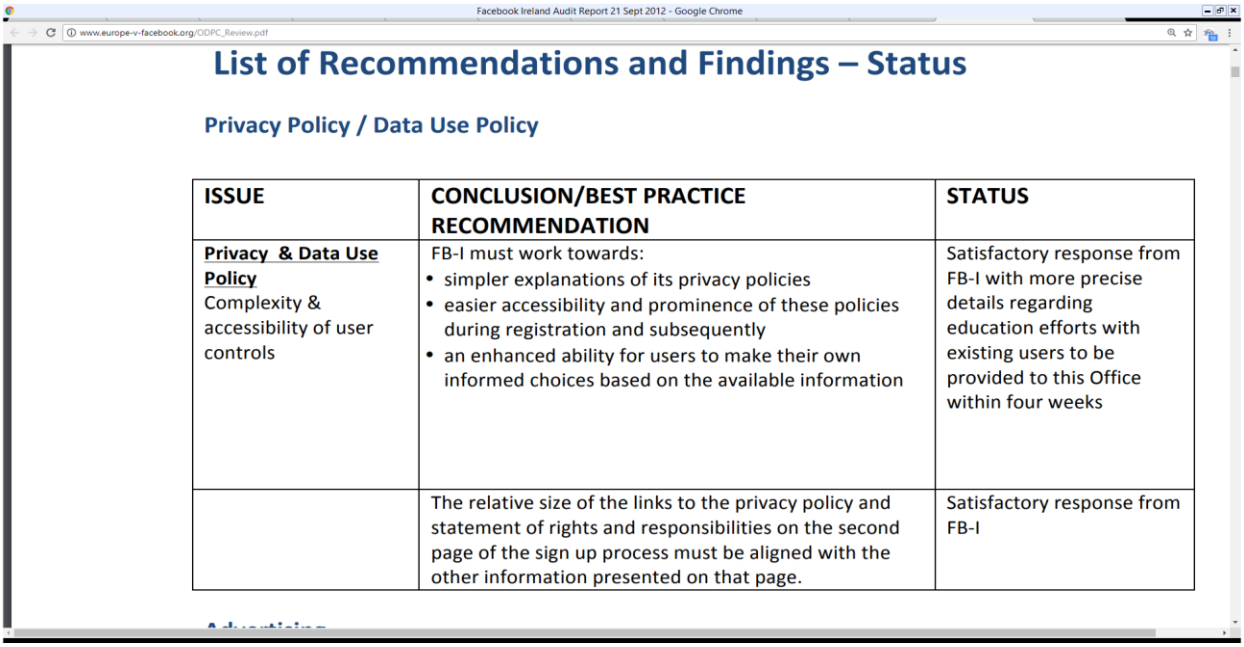
3

will be necessary as it continues to bring forward new innovations. The value of such engagement to identify and deal with any data protection concerns prior to launch is fully accepted by FB-I. Such discussion is also necessary in relation to new issues that arose in the course of the review – for example, the balance to be struck between FB-I's duty to protect young users from sexual predators, through monitoring certain user behaviour and reporting reasonable suspicions to relevant authorities, and the need to ensure that such monitoring and reporting is proportionate to the danger of serious consequences for young victims.

It is clear that this Review is no more than an assessment at a point in time of FB-I's compliance with its data protection obligations to its users. As indicated above new developments in terms of services to users and use of their data for advertising purposes will continue to throw up challenges to FB-I's strengthened in-house compliance function. It will also involve continued detailed involvement of our Office's oversight role, including responding to issues raised by other DPAs and by the many data subjects for whom FB-I is the data controller.

Report, pp. 3-4.

91. The ODPC's Report (at page 7) issued the following "Recommendations and Findings" relative to Facebook Ireland's "Privacy Policy/Data Use Policy":


Facebook Ireland Audit Report 21 Sept 2012 - Google Chrome

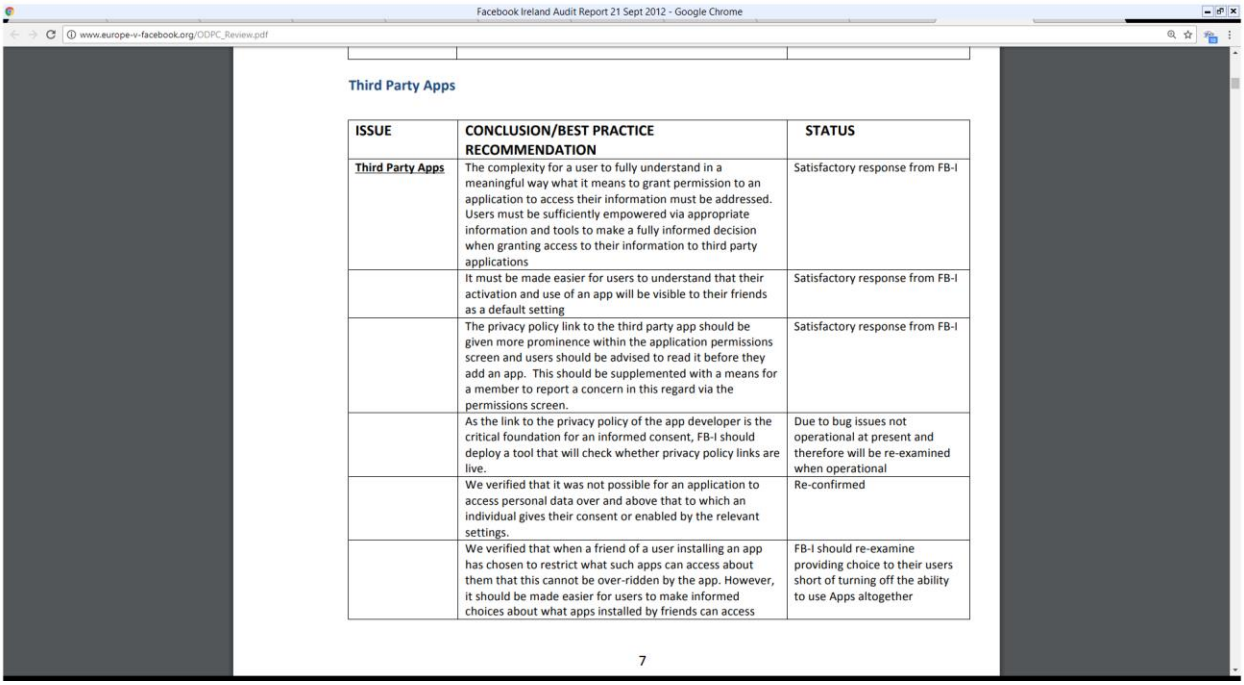
www.europe-v-facebook.org/ODPC_Review.pdf

List of Recommendations and Findings – Status

Privacy Policy / Data Use Policy

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Privacy & Data Use Policy Complexity & accessibility of user controls	FB-I must work towards: • simpler explanations of its privacy policies • easier accessibility and prominence of these policies during registration and subsequently • an enhanced ability for users to make their own informed choices based on the available information	Satisfactory response from FB-I with more precise details regarding education efforts with existing users to be provided to this Office within four weeks
	The relative size of the links to the privacy policy and statement of rights and responsibilities on the second page of the sign up process must be aligned with the other information presented on that page.	Satisfactory response from FB-I

92. The ODPC's Report issued the following "Recommendations and Findings" relative to Facebook Ireland's "Third Party Apps":

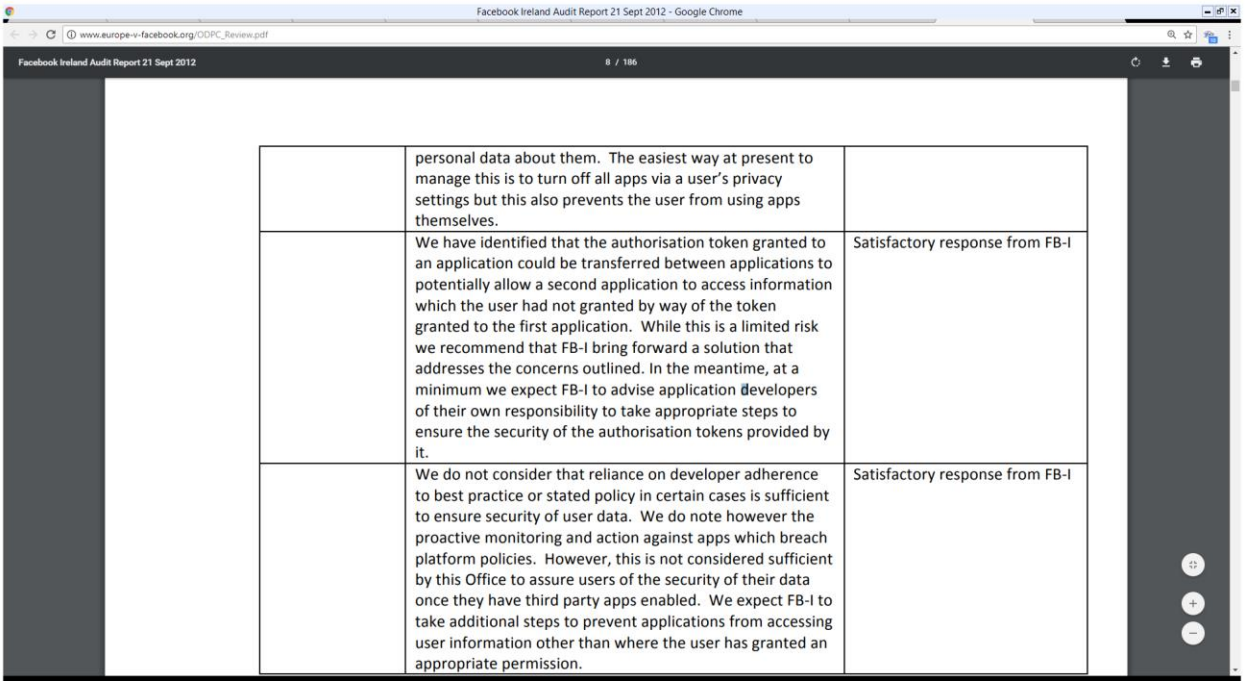

Facebook Ireland Audit Report 21 Sept 2012 - Google Chrome

www.europe-v-facebook.org/ODPC_Review.pdf

Third Party Apps

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Third Party Apps	The complexity for a user to fully understand in a meaningful way what it means to grant permission to an application to access their information must be addressed. Users must be sufficiently empowered via appropriate information and tools to make a fully informed decision when granting access to their information to third party applications	Satisfactory response from FB-I
	It must be made easier for users to understand that their activation and use of an app will be visible to their friends as a default setting	Satisfactory response from FB-I
	The privacy policy link to the third party app should be given more prominence within the application permissions screen and users should be advised to read it before they add an app. This should be supplemented with a means for a member to report a concern in this regard via the permissions screen.	Satisfactory response from FB-I
	As the link to the privacy policy of the app developer is the critical foundation for an informed consent, FB-I should deploy a tool that will check whether privacy policy links are live.	Due to bug issues not operational at present and therefore will be re-examined when operational
	We verified that it was not possible for an application to access personal data over and above that to which an individual gives their consent or enabled by the relevant settings.	Re-confirmed
	We verified that when a friend of a user installing an app has chosen to restrict what such apps can access about them that this cannot be over-ridden by the app. However, it should be made easier for users to make informed choices about what apps installed by friends can access	FB-I should re-examine providing choice to their users short of turning off the ability to use Apps altogether

7



	personal data about them. The easiest way at present to manage this is to turn off all apps via a user's privacy settings but this also prevents the user from using apps themselves.	
	We have identified that the authorisation token granted to an application could be transferred between applications to potentially allow a second application to access information which the user had not granted by way of the token granted to the first application. While this is a limited risk we recommend that FB-I bring forward a solution that addresses the concerns outlined. In the meantime, at a minimum we expect FB-I to advise application developers of their own responsibility to take appropriate steps to ensure the security of the authorisation tokens provided by it.	Satisfactory response from FB-I
	We do not consider that reliance on developer adherence to best practice or stated policy in certain cases is sufficient to ensure security of user data. We do note however the proactive monitoring and action against apps which breach platform policies. However, this is not considered sufficient by this Office to assure users of the security of their data once they have third party apps enabled. We expect FB-I to take additional steps to prevent applications from accessing user information other than where the user has granted an appropriate permission.	Satisfactory response from FB-I

93. ODPC's Report recommended that "Users must be sufficiently empowered via appropriate information and tools to make a fully informed decision when granting access to their information to third party applications." Report at p. 7.

94. The Report also recommended that "[i]t must be easier for users to understand that their activation and use of an app will be visible to their friends as a default setting." *Id.*

95. The Report stated that "the link to the privacy policy of the app developer is the critical foundation for an informed consent, FB-1 should deploy a tool that will check whether privacy links are live." *Id.*

96. The Report stated that "it should be easier for users to make informed choices about what apps installed by friends can access personal data about them." *Id.*

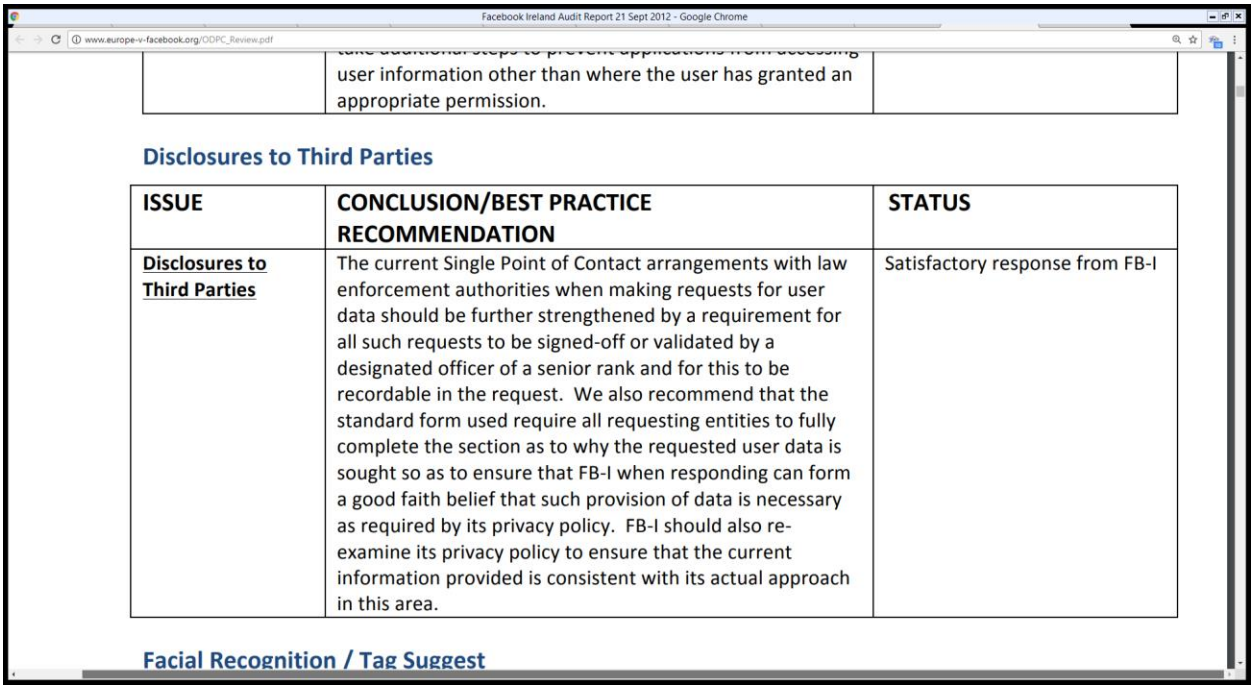
97. The Report said that Facebook Ireland should "re-examine providing choice to their users short of turning off the ability of use Apps together." *Id.*

98. The Report "verified" whether it was "possible for an application to access personal data over and above that to which an individual gives their consent or enabled by the relevant settings." *Id.*

99. The Report also "verified" "that when a friend of a user installing an app has chosen to restrict what such apps can access about them . . . cannot be over-ridden by the app."

100. While the Report "verified" these tests, the Report and the object of the tests put Defendants Zuckerberg and Facebook on notice for the risk that apps may take efforts to over-ride user settings or "access personal data over and above that to which an individual givers their consent or enabled by the relevant settings."

101. The Report (at page 8) issued the following "CONCLUSION/BEST PRACTICE RECOMMENDATION" relative to Facebook Ireland's "Disclosures to Third Parties":



Facebook Ireland Audit Report 21 Sept 2012 - Google Chrome

www.europe-v-facebook.org/ODPC_Review.pdf

	user information other than where the user has granted an appropriate permission.	

Disclosures to Third Parties

ISSUE	CONCLUSION/BEST PRACTICE RECOMMENDATION	STATUS
Disclosures to Third Parties	The current Single Point of Contact arrangements with law enforcement authorities when making requests for user data should be further strengthened by a requirement for all such requests to be signed-off or validated by a designated officer of a senior rank and for this to be recordable in the request. We also recommend that the standard form used require all requesting entities to fully complete the section as to why the requested user data is sought so as to ensure that FB-I when responding can form a good faith belief that such provision of data is necessary as required by its privacy policy. FB-I should also re-examine its privacy policy to ensure that the current information provided is consistent with its actual approach in this area.	Satisfactory response from FB-I

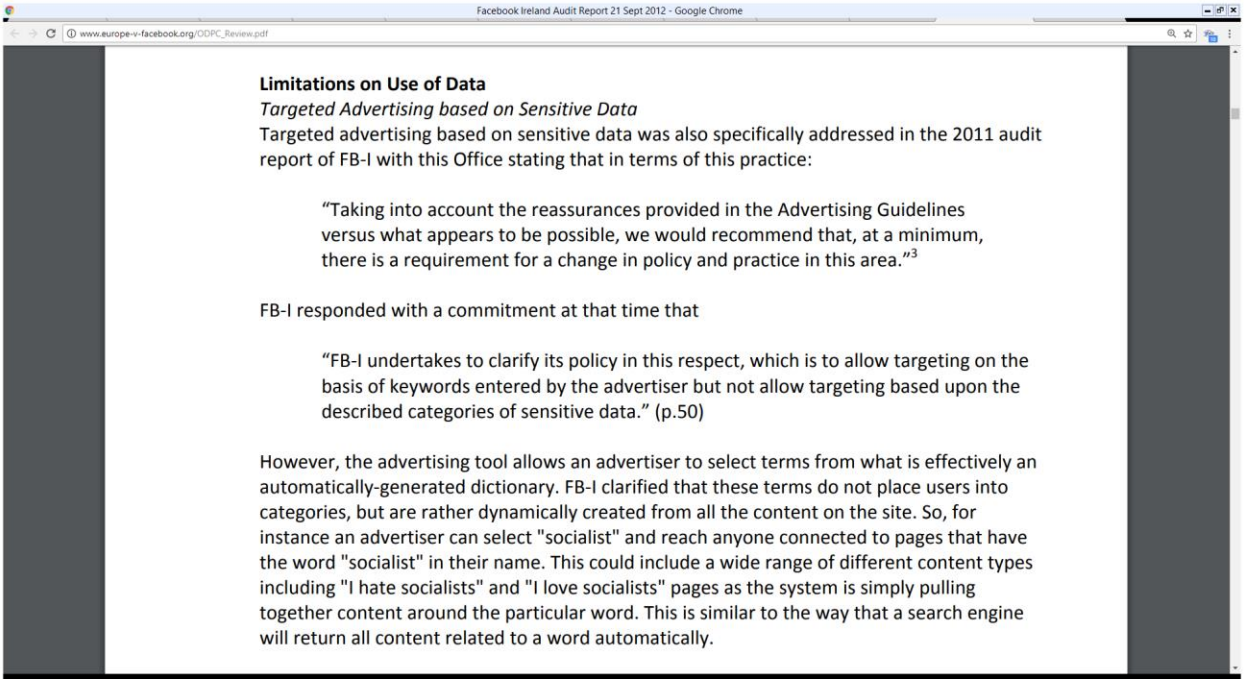
Facial Recognition / Tag Suggest

102. In particular, the Report recommended that Facebook Ireland take measures to "ensure that FB-1 . . . can form a good faith belief that such provision of data is necessary as required by its privacy policy." See page 8 of Report.

103. The Report also recommended that Facebook Ireland "should reexamine its privacy policy to ensure that current information provided is consistent with its actual approach to this area." *Id.*

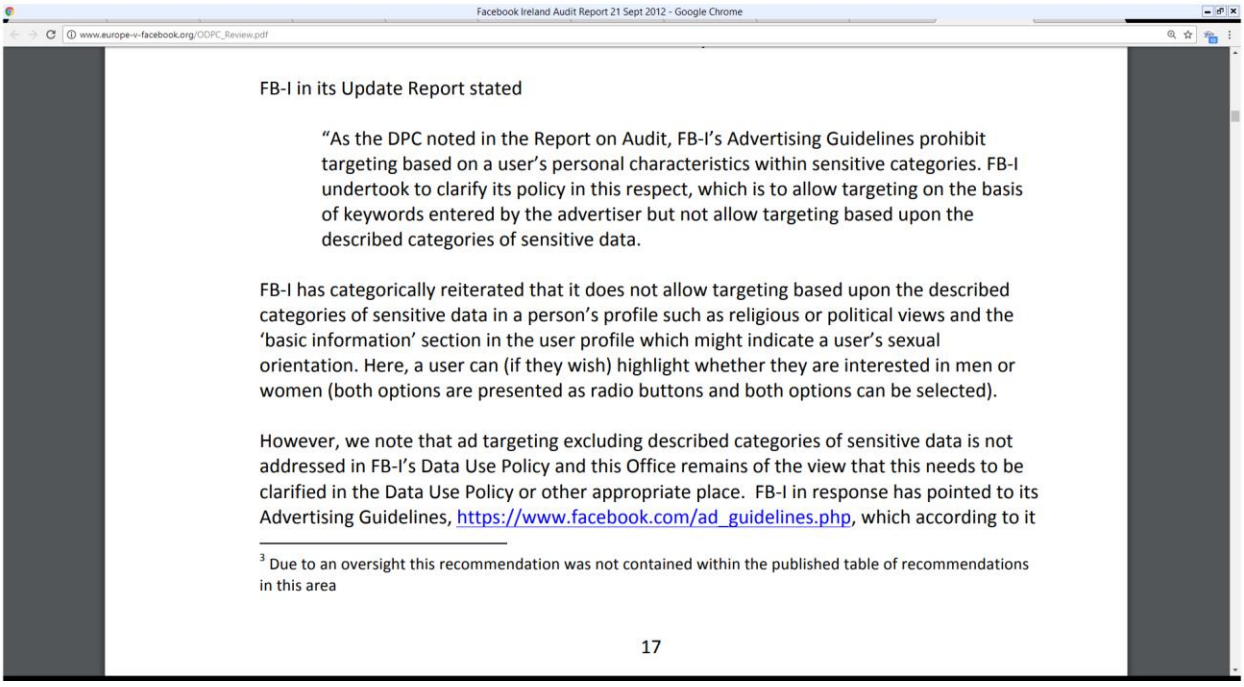
104. The Report focused on the topic of "Advertising" and said the following, noting Facebook Ireland "has accelerated the pace of innovation in relation to advertising." Report at p. 15.

105. The Report focused on the topic of "Limitations on Use of Data" and the sub-topic of "*Targeted Advertising based on Sensitive Data*" and made an example of "targeted" advertising whereby an advertising transmitted adds to users if the users included the word "socialist" in their profile:



Report at p. 17.

106. The Report quoted from Facebook Europe's "Updated Report" which highlighted Facebook Europe's "clarify[ied] policy in this respect" and criticized Facebook Ireland's "Updated Report" as follows:


Facebook Ireland Audit Report 21 Sept 2012 - Google Chrome

www.europe-v-facebook.org/ODPC_Review.pdf

FB-I in its Update Report stated

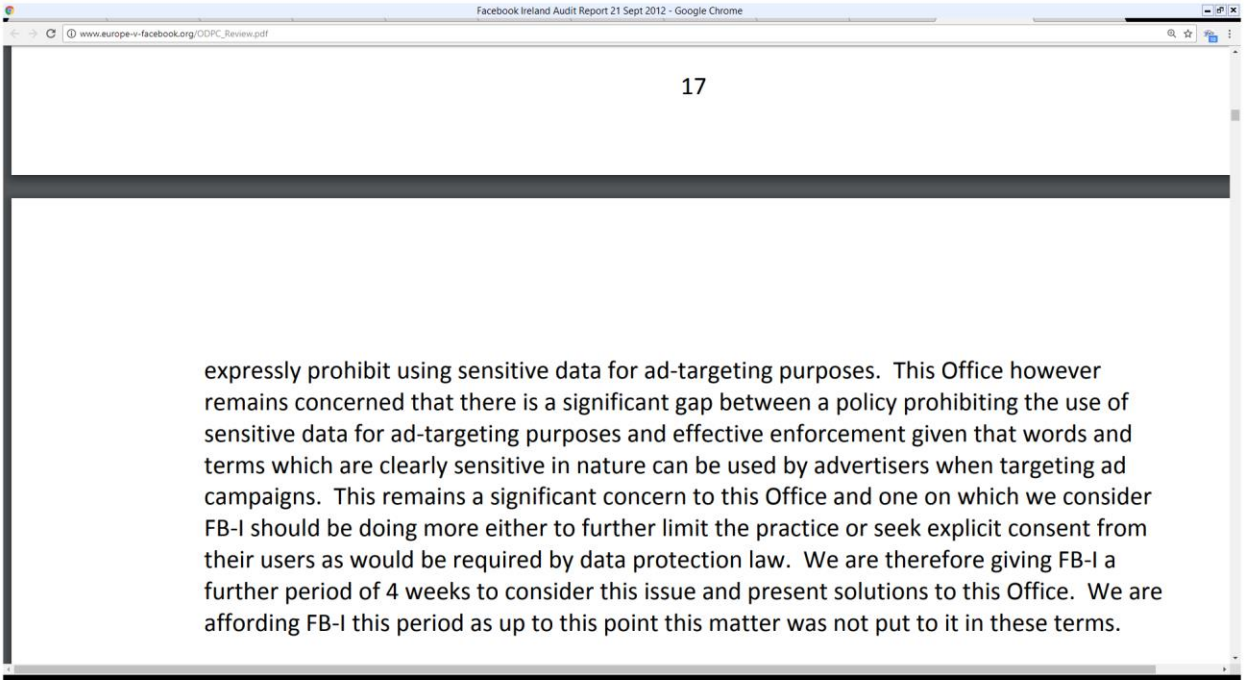
> "As the DPC noted in the Report on Audit, FB-I's Advertising Guidelines prohibit targeting based on a user's personal characteristics within sensitive categories. FB-I undertook to clarify its policy in this respect, which is to allow targeting on the basis of keywords entered by the advertiser but not allow targeting based upon the described categories of sensitive data.

FB-I has categorically reiterated that it does not allow targeting based upon the described categories of sensitive data in a person's profile such as religious or political views and the 'basic information' section in the user profile which might indicate a user's sexual orientation. Here, a user can (if they wish) highlight whether they are interested in men or women (both options are presented as radio buttons and both options can be selected).

However, we note that ad targeting excluding described categories of sensitive data is not addressed in FB-I's Data Use Policy and this Office remains of the view that this needs to be clarified in the Data Use Policy or other appropriate place. FB-I in response has pointed to its Advertising Guidelines, https://www.facebook.com/ad_guidelines.php, which according to it

[3] Due to an oversight this recommendation was not contained within the published table of recommendations in this area

17

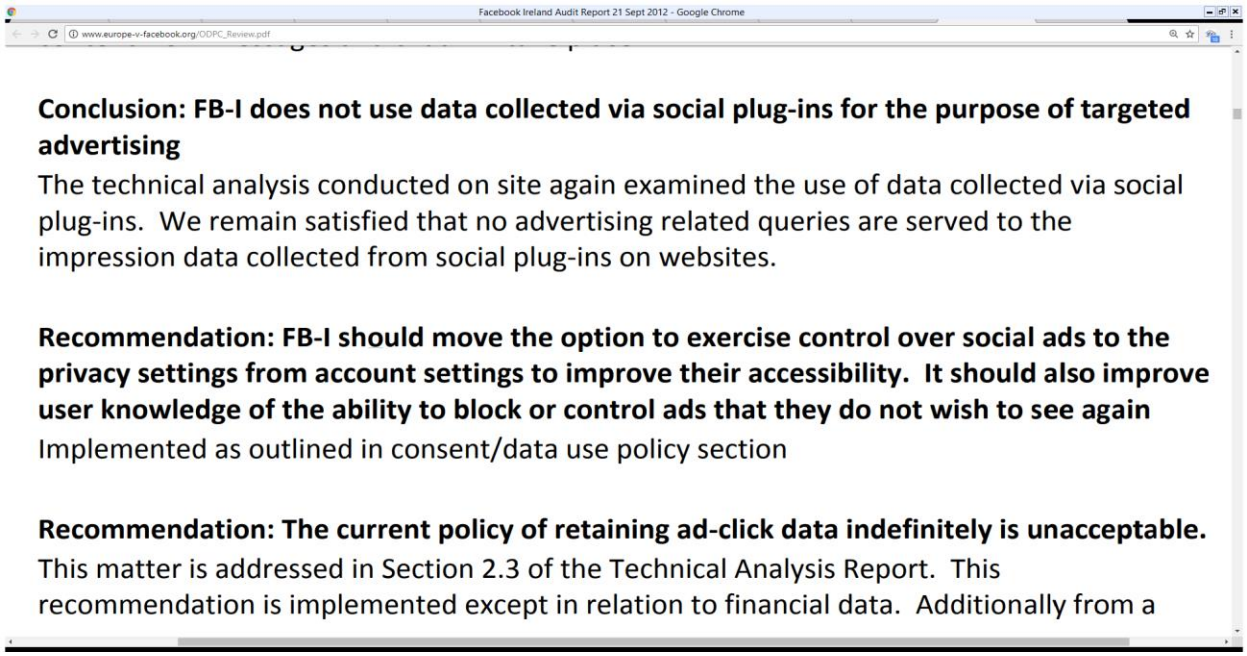

Facebook Ireland Audit Report 21 Sept 2012 - Google Chrome

www.europe-v-facebook.org/ODPC_Review.pdf

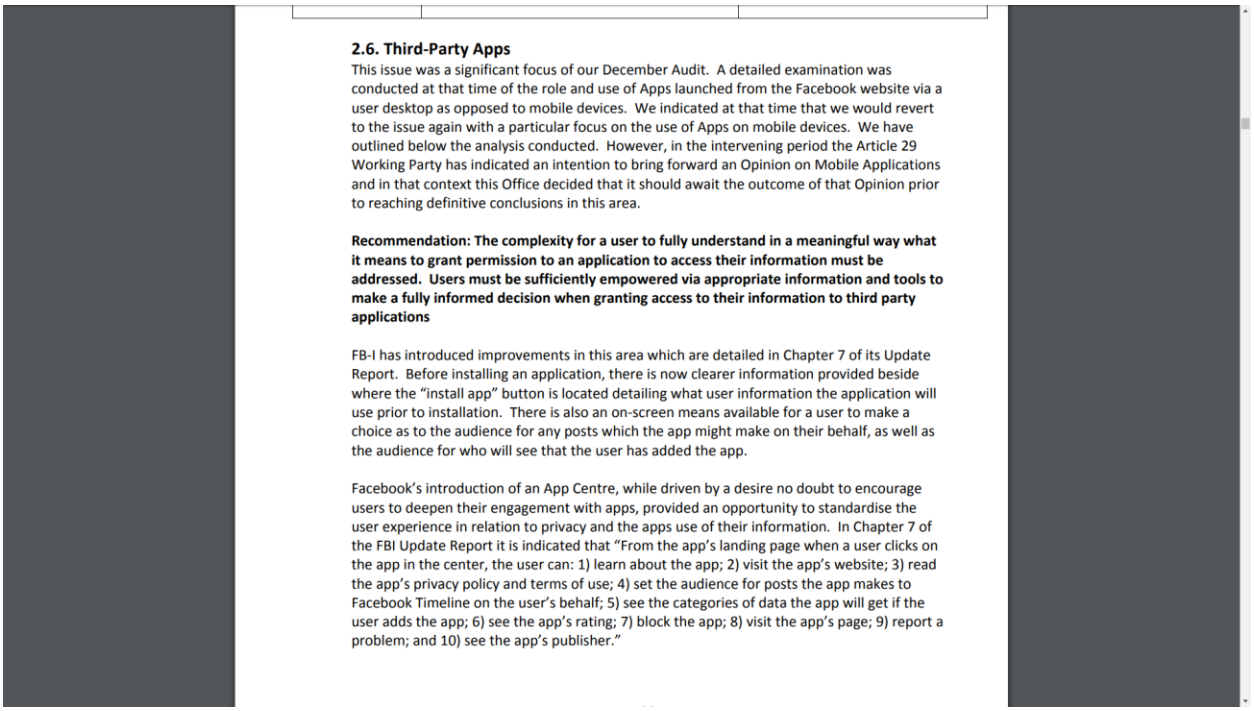
17

expressly prohibit using sensitive data for ad-targeting purposes. This Office however remains concerned that there is a significant gap between a policy prohibiting the use of sensitive data for ad-targeting purposes and effective enforcement given that words and terms which are clearly sensitive in nature can be used by advertisers when targeting ad campaigns. This remains a significant concern to this Office and one on which we consider FB-I should be doing more either to further limit the practice or seek explicit consent from their users as would be required by data protection law. We are therefore giving FB-I a further period of 4 weeks to consider this issue and present solutions to this Office. We are affording FB-I this period as up to this point this matter was not put to it in these terms.

107. While the Report found that Facebook Ireland did "not use data collected via social plug-ins for the purpose of targeted advertising", its investigation put Defendants Zuckerberg and Facebook on notice of this issue, and Report made the below identified recommendations to allow users to "block or control adds that they do not wish to see again":



108. The Report noted that "Third-Party Apps" was a "significant focus" of a recent Audit and made following recommendations relative to "Third-Party Apps" as depicted below:



2.6. Third-Party Apps

This issue was a significant focus of our December Audit. A detailed examination was conducted at that time of the role and use of Apps launched from the Facebook website via a user desktop as opposed to mobile devices. We indicated at that time that we would revert to the issue again with a particular focus on the use of Apps on mobile devices. We have outlined below the analysis conducted. However, in the intervening period the Article 29 Working Party has indicated an intention to bring forward an Opinion on Mobile Applications and in that context this Office decided that it should await the outcome of that Opinion prior to reaching definitive conclusions in this area.

Recommendation: The complexity for a user to fully understand in a meaningful way what it means to grant permission to an application to access their information must be addressed. Users must be sufficiently empowered via appropriate information and tools to make a fully informed decision when granting access to their information to third party applications

FB-I has introduced improvements in this area which are detailed in Chapter 7 of its Update Report. Before installing an application, there is now clearer information provided beside where the "install app" button is located detailing what user information the application will use prior to installation. There is also an on-screen means available for a user to make a choice as to the audience for any posts which the app might make on their behalf, as well as the audience for who will see that the user has added the app.

Facebook's introduction of an App Centre, while driven by a desire no doubt to encourage users to deepen their engagement with apps, provided an opportunity to standardise the user experience in relation to privacy and the apps use of their information. In Chapter 7 of the FBI Update Report it is indicated that "From the app's landing page when a user clicks on the app in the center, the user can: 1) learn about the app; 2) visit the app's website; 3) read the app's privacy policy and terms of use; 4) set the audience for posts the app makes to Facebook Timeline on the user's behalf; 5) see the categories of data the app will get if the user adds the app; 6) see the app's rating; 7) block the app; 8) visit the app's page; 9) report a problem; and 10) see the app's publisher."

109. On information and belief, Facebook and Zuckerman and as yet unknown Facebook executives had access to and were made aware of the ODP Report, but they chose not implement one or more of ODPC's suggested reforms.

110. In particular, Ms. Tassi, as Facebooks' head privacy counsel, she was deeply involved in Facebook Ireland's response ODPC's investigation and audit.

111. On information and belief, Tassi declined to implement one or more of ODPC's suggested reforms.

112. Had Tassi, Facebook and Zuckerman and as yet unknown Facebook executives implemented ODPC's suggested reforms, the misconduct committed by Cambridge and various unknown John and Jane Doe Defendants and Doe Defendant Entities may not have occurred.

113. Had Tassi, Facebook and Zuckerman and as yet unknown Facebook executives implemented ODPC's suggested reforms, the misconduct committed by Cambridge and various unknown John and Jane Doe Defendants and Doe Defendant

Entities may not have occurred *and the* U.S. Presidential election may have resulted in a different victor.

114. As explained by Will Bunch of *The Inquirer*:

> Trump's announcement launched a mystery that's lasted 14 months into the most unlikely presidency in American history. Where did the ideas that animated the candidate's packed rallies — and juiced voter turnout in Rust Belt states like Pennsylvania, Michigan, Wisconsin and Ohio — come from? "Build the wall!"? "Drain the swamp!"? "Crooked Hillary!"? "Deep state!"? Defining immigrants as violent gangs or murderous thugs? Painting American's urban neighborhoods as crime-infested ratholes.
>
> In a stunning week of revelations, we now know the answer. The core messages of the president's underlying xenophobia and racism that animated his base didn't emerge from the mind of "very stable genius" Trump (despite a long life of troubling racial attitudes). Instead, the nonstop undercurrent of hate toward The Other in American life was focus-grouped, computer-coded, deliberately amplified by a new ultra-right-wing media echo chamber and then targeted with cruise-missile precision at the handful of states that Trump won by roughly 100,000 votes to grab the Electoral College.
>
> * * *
>
> We know now how this worked, thanks to a courageous insider, Christopher Wylie, who has revealed the secrets of Bannon and Cambridge Analytica as a whistleblower. Much of the attention has focused, understandably, on what you might call the "garbage in" aspect of CA's work for Trump, the fraud and trickery that was used to gain 50 million Facebook profiles and use "psychometric" profiling to play on voters' fears and prejudices. There's been way too little focus on the "garbage out" — what those messages were and how they were crafted.
>
> Wylie told the Washington Post the backstory of how he, Bannon, a financier then running the right-wing Breitbart News, ultra-conservative hedge-fund billionaire Robert Mercer and a cyber-warfare expert named Alexander Nix came together in 2014 to launch Cambridge Analytica. The whistleblower said it was Bannon who was calling the shots and who was particularly interested in one particular issue: How to win over young conservative white males who were staying home on Election Day. The new start-up convened focus groups to find out.

http://www.philly.com/philly/columnists/will_bunch/race-realism-steve-bannon-cambridge-analytica-elected-trump-20180322.html

115. While *MyDigitalLife* was a third-party app, Facebook had a duty and obligation to ensure that *MyDigitalLife* was not improperly mining and misusing the personal information of Facebook users.

116. As a result of Cambridge's misconduct and Facebook's negligence or recklessness, Plaintiff and millions of other Facebook users were improperly barraged with manipulated data, stories, advertisements and posts, all (wrongly) intended to influence their votes in the 2016 Presidential Election.

117. Facebook owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, safeguarding, and/or obtaining their Personal Information.

ADDITIONAL ALLEGATIONS

118. Plaintiffs do not recall downloading the *MyDigitalLife* app.

119. Nevertheless, Plaintiffs and similarly situated Class Members were harmed by the misconduct of Cambridge, Facebook and the John Does Defendants to the extent that they had their personal information mined as a result of another Facebook "friend" downloading and using the *MyDigitalLife* app.

120. Plaintiffs and similarly situated Class Members were harmed by the misconduct of Cambridge, Facebook and the John Does Defendants to the extent that they had their were improperly bombarded with specifically targeted posts, messages, advertisements and other data promoting Donald Trump as a result of another Facebook "friend" downloading and using the *MyDigitalLife* app. and having the resultant data mined and manipulated by Cambridge and the John Does Defendants.

121. Plaintiffs and similarly situated Class Members were harmed by the misconduct of Cambridge, Facebook and the John Does Defendants to the extent that they had their were improperly bombarded with specifically targeted posts, messages,

advertisements and other data promoting criticizing Hillary Clinton as a result of another Facebook "friend" downloading and using the *MyDigitalLife* app. and having the resultant data mined and manipulated by Cambridge and the John Does Defendants.

122. Plaintiffs and similarly situated Class Members were harmed by the misconduct of Cambridge, Facebook and the John Does Defendants to the extent that they had their were improperly bombarded with specifically targeted posts, messages, advertisements and other data which essentially created "fake news" to make Hillary Clinton look like a bad presidential candidate.

123. Plaintiffs and similarly situated Class Members were harmed by the misconduct of Cambridge, Facebook and the John Does Defendants to the extent that they had their were improperly bombarded with specifically targeted posts, messages, advertisements and other data which essentially created "fake news" to make Donald Trump look like a good presidential candidate.

124. As result of the misconduct of Cambridge, Facebook and the John Does Defendants, Plaintiffs and similarly situated Class Members were harmed because the above misconduct helped influence voters to vote for Donald Trump.

125. As result of the misconduct of Cambridge, Facebook and the John Does Defendants, Plaintiffs and similarly situated Class Members were harmed because the above misconduct forced them to endure targeted posts, messages, advertisements and other data which essentially created "fake news" which resulted in wasted battery life and data usage on their smart phones.

126. As discussed below in the various Counts, Plaintiffs and the Class Members are entitled to declaratory relief, equitable and injunctive relief and restitution.

COUNT I

Violation of §§ 2511(1)(a) & (1)(d) of the ECPA (the Wiretap Act)

127. Plaintiffs adopt and incorporate each and every allegation of this complaint as if stated fully herein.

128. Plaintiffs, individually and on behalf of Class Members, assert violations of 18 U.S.C. §§ 2511(1)(a) and (1)(d)

129. In 1986, Congress passed the ECPA with the express purpose of affording to electronic communications, such as the private online communications at issue here, the same protections that attach to private letters sent via the U.S. Postal Service. In recommending adoption of the ECPA, the Senate Committee on the Judiciary issued the following statement:

> A letter sent by first class mail is afforded a high level of protection against unauthorized opening by a combination of constitutional provisions, case law, and U.S. Postal Service statutes and regulations. Voice communications transmitted via common carrier are protected by title III of the Omnibus Crime Control and Safe Streets Act of 1968. But there are no comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology. This is so, even though American citizens and American businesses are using these new forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services.

130. The Senator who introduced the Electronic Communications Privacy Act to Congress described its overarching goal as follows: "We cannot let any American feel less confident in putting information into an electronic mail network than he or she would in putting it into an envelope and dropping it off at the Post Office."

131. Defendants are persons under the Wiretap Act pursuant to 18 U.S.C. § 2510(6).

132. The Wiretap Act provides a private right of action against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to

intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a).

133. Electronic communication is "any transfer of signs, signals, writing, images, sound, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate or foreign commerce...." 18 U.S.C. § 2510(12).

134. The named Plaintiffs' usage of Facebook to interact with "friends" (via direct messages and on-line posts) is a form of an electronic communication because in using the Facebook app the named Plaintiffs transferred and exchanged personal information with "friends" through the Facebook app.

135. The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Id.§ 2510(4).

136. As set forth above Defendants Zuckerberg and Facebook allowed Cambridge to unlawfully capture and/or intercept sensitive personal information exchanged between friends and from on-line postings (communications) between friends related to the 2016 Presidential Election.

137. Section 2520(a) of the Wiretap Act states that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity . . . which engaged in that violation such relief as may be appropriate."

138. Section 2520(b) of the Wiretap Act states as follows:

Relief.--In an action under this section, appropriate relief includes—

> (1) such preliminary and other equitable or declaratory relief as may be appropriate;
> (2) damages under subsection (c) and punitive damages in appropriate cases; and

> (3) a reasonable attorney's fee and other litigation costs reasonably incurred.

139. Section 2520(c)(2) of the Wiretap Act states that a "court may assess as damages whichever is the greater of—

> (A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or
> (B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

140. The Wiretap Act does not require a showing of actual harm.

141. Under the Wiretap Act, a plaintiff may recover either actual damages, statutory damages, or injunctive relief. 18 U.S.C. § 2520(b), (c)(2).

142. In light of the above factual allegations, and the admissions of Defendants, sensitive personal data was unlawfully captured by Cambridge.

143. Section 2511(1)(a) of the Wiretap Act provides a private right of action against any person who:

> . . . intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication.

144. Plaintiffs and the putative class members have been damaged by virtue of the fact that their sensitive personal information (has been knowingly or recklessly been captured and misused by Cambridge in violation of Section 2511(1)(a) of the Wiretap Act - in the absence of a lawful or legitimate business reason.

145. Section 2512(1)(b) of the Wiretap Act also provides a private right of action against any person who

> . . . intentionally . . . (b) manufactures, assembles, possesses, or sells any electronic . . . or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of . . . electronic communications . . . .

146. Facebook utilized unlawful devices and/or technology for the purpose of acquiring user content (electronic communications), postings, direct messages of the Plaintiffs and Class Members in the course of the transmission of this user content to other users.

147. Alternatively, Cambridge utilized unlawful devices and/or technology for the purpose of acquiring user content (electronic communications), postings, direct messages of the Plaintiffs and Class Members in the course of the transmission of this user content to other users.

148. On information and belief, such devices or technology include, but are not limited to, web crawlers and social plugins.

149. Pursuant to 18 U.S.C. § 2511(1)(a), Facebook intentionally intercepted, intercepts, or endeavored or endeavors to intercept the electronic communications of Plaintiffs and Class Members and provided those communications to Cambridge without the permission of and unbeknownst to Plaintiffs to allow Cambridge to influence the 2016 Presidential Election without the permission of and unbeknownst to Plaintiffs.

150. Alternatively, pursuant to 18 U.S.C. § 2511(1)(a), Cambridge intentionally intercepted, intercepts, or endeavored or endeavors to intercept the electronic communications of Plaintiffs and Class Members and misused these communications to help influence the 2016 Presidential Election without the permission of and unbeknownst to Plaintiffs.

151. The devices or technology were not used by Facebook or Cambridge, operating as electronic communication services, in the ordinary course of business as providers of electronic communication services.

152. On information and belief, Facebook unlawfully intercepted electronic communications sent by and to Plaintiffs and Class Members for the purpose of

generating income from third-parties like Cambridge. This conduct was not within the ordinary course of business of a provider of an electronic communication service.

153. On information and belief, Facebook unlawfully intercepted electronic communications sent by and to Plaintiffs and Class Members for the purposes of cataloging user data and did so in violation of its user agreements, its public statements to users and in violation of federal and state law. This conduct was not within the ordinary course of business of a provider of an electronic communication service.

154. On information and belief, Facebook unlawfully intercepted electronic communications sent by and to Plaintiffs and Class Members for the purposes of cataloging user data and did so in violation of the property rights of Plaintiffs and Class Members, and third parties. This conduct was not within the ordinary course of business of a provider of an electronic communication service.

155. Pursuant to 18 U.S.C. § 2511(1)(d), Facebook intentionally used, uses, or endeavored or endeavors to use the contents of Plaintiffs' and Class Members' electronic communications while knowing or having reason to know that it obtained the information through the interception of the electronic communication in violation of 18 U.S.C. § 2511(1)(a).

156. Facebook's interception of and use of the contents of Plaintiffs' and Class Members' electronic communications were not performed by any employees engaged in any activity necessary for the rendition of an electronic communication service or for the protection of the rights or property of Facebook or Cambridge.

157. Alternatively, Cambridge's interception of and use of the contents of Plaintiffs' and Class Members' electronic communications were not performed by any employees engaged in any activity necessary for the rendition of an electronic

communication service or for the protection of the rights or property of Facebook or Cambridge.

158. Plaintiffs did not consent to Facebook's interception or use of the contents of the electronic communications.

159. Alternatively, Plaintiffs did not consent to Cambridge's interception or use of the contents of the electronic communications.

160. Defendant Zuckerman is a "person" under the Wiretap Act also liable for any violations of the Act because he was on notice of Facebook's shortcomings relative to the protection of user's privacy.

161. Further, on information and belief, Defendant Zuckerman knew of Cambridge's unlawful scheme and did nothing to prevent Cambridge from unlawfully obtaining Plaintiffs' and Class Member's sensitive personal information.

WHEREFORE as a result of Defendants' violations of § 2511, pursuant to § 2520, Plaintiffs and the class they seek to represent have been harmed by Defendants' misconduct and are entitled to statutory damages, actual damages and reasonable attorney's fees and costs, as well as declaratory and injunctive relief.

COUNT II

Violations of the Stored Communications Act, 18 U.S.C. § 2701, *et seq*.

162. Plaintiffs adopt and incorporate each and every allegation of this complaint as if stated fully herein.

163. Facebook and/or Cambridge are electronic communications providers within the meaning of the Stored Communications Act.

164. Under the Stored Communications Act, an entity providing an electronic communication service to the public "shall not knowingly divulge to any person or entity

the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

165. Section 2701(a)(1) of the Stored Communications Act authorizes a private right of action for damages, injunctive relief and equitable relief against any person who "intentionally exceeds an authorization to access [a facility through which an electronic communication service is provided] . . . and thereby obtains . . . access to wire or electronic communication while it is in electronic storage in such system . . . ."

166. Facebook and Cambridge intentionally exceeded any authorization they may have had to Plaintiffs' and other users' stored electronic communications by allowing Cambridge to have access to Plaintiffs' and other users' stored electronic communications which also contained sensitive personal information.

167. Facebook and Cambridge knowingly allowed Cambridge and as yet unknown third parties to intentionally exceed any authorization it may have had to Plaintiffs' and other users' stored electronic communications.

168. Defendant Zuckerman is a "person" under the Stored Communications Act also liable for any violations of the Act because he was on notice of Facebook's shortcomings relative to the protection of user's privacy.

169. Further, on information and belief, Defendant Zuckerman knew of Cambridge's unlawful scheme and did nothing to prevent Cambridge from unlawfully obtaining Plaintiffs' and Class Member's sensitive personal information.

170. Plaintiffs reserve the right to amend this Count to include as yet unknown John and Jane Doe Defendants employed by and/or associated with Facebook.

171. Plaintiffs have been damaged by Defendants' misconduct which improperly influenced the 2016 Presidential Election, resulting in the election of the current President.

WHEREFORE, as set forth above, Plaintiffs and the nationwide class they seek to represent have been harmed by Defendants' misconduct and are entitled to statutory damages, actual damages and reasonable attorney's fees and costs, as well as declaratory and injunctive relief.

COUNT III

Common Law Negligence

172. Plaintiffs adopt and incorporate each and every allegation of this complaint as if stated fully herein.

173. Facebook knew and knows that Facebook users consider their personal information to be sensitive and valuable.

174. Plaintiffs entrusted Facebook to safeguard their personal information.

175. Plaintiffs had no reason to believe that Facebook would allow their sensitive personal information to be mined, shared or exploited with third-parties like Cambridge and organizations managed by Mr. Bannon and the Mercers.

176. Plaintiffs had no reason to believe that Facebook would allow their news feeds and interactions with friends to be infiltrated by third-parties like Cambridge and organizations managed by Mr. Bannon and the Mercers and other as yet unknown John and Jane Does.

177. Facebook and its CEO Zuckerberg owed a duty to Plaintiffs to exercise reasonable care in obtaining and protecting their personal information, and keeping it from being compromised, lost, stolen, misused, and or/disclosed to third-parties like Cambridge and organizations managed by Mr. Bannon and the Mercers and other as yet unknown John and Jane Does.

178. Accordingly, Facebook and Zuckerberg entered into a special relationship with Plaintiffs.

179. Plaintiffs reasonably believed that Facebook and Zuckerberg would take appropriate measures to protect their personal information based up on historical postings and disclosures by both Facebook and Zuckerberg.

180. Plaintiffs reasonably believed that Facebook and Zuckerberg would inform them of misuse of user information by a third-party based up on historical postings and disclosures by both Facebook and Zuckerberg.

181. Facebook and Zuckerberg (and unknown John and Jane Doe Defendants employed by and/or associated with Facebook) breached their duties to Plaintiffs and Class Members by failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs and Class Members' personal information from authorized access.

182. Facebook and Zuckerberg (and unknown John and Jane Doe Defendants employed by and/or associated with Facebook) breached their duty to timely disclose to Plaintiffs and Class Members that their personal information had been improperly obtained by Cambridge and as yet unknown John and Jane Doe Defendants.

183. But for Zuckerberg and Facebook's wrongful and negligent breach of their duties owed to Plaintiffs and the Class Members (including breach by as yet unknown John and Jane Doe Defendants employed by and/or associated with Facebook), the personal information of Plaintiffs and the Class Members would not have been improperly obtained by Cambridge and as yet unknown John and Jane Doe Defendants.

184. Facebook's negligence was a direct and proximate cause of the misappropriate of the personal information of Plaintiffs and the Class Members.

185. Plaintiffs reserve the right to amend this Count to include as yet unknown John and Jane Doe Defendants employed by and/or associated with Facebook.

186. Plaintiffs seek damages which are directly resulted from Facebook allowing Cambridge to improperly influence the 2016 Presidential Election, resulting in the election of the current President.

WHEREFORE, Plaintiffs and nationwide class of Facebook users are entitled to damages, injunctive relief and equitable relief to remedy the above described misconduct.

COUNT IV

Breach of Contract

187. Plaintiffs adopt and incorporate each and every allegation of this complaint as if stated fully herein.

188. In order to register as a user of Facebook, Plaintiffs and the Class affirmatively assent to its Terms and Conditions and Privacy Policy (the "Agreement").

189. The Agreement's provisions constitute a valid and enforceable contract between Plaintiffs and the Class on the one hand, and Facebook on the other.

190. Under the Agreement, Plaintiffs and the Class transmitted sensitive personally identifiable information to Facebook in exchange for use of Facebook and Facebook's promise that it would not share that personal information with third parties, including but not limited to advertisers, without their authorization.

191. Facebook users effectively pay for Facebook's services through their provision of their sensitive personal information into Facebook's safekeeping.

192. Facebook's users exchange something valuable, providing Facebook with access to their sensitive personal information, and in return, Facebook's users obtain access Facebook's services.

193. A material consideration for Plaintiffs' transmission of their sensitive personal information to Facebook is Facebook's promise to safeguard their sensitive personal information.

194. In particular, Facebook promised that any personal information submitted by its users will only be disclosed to other users and third-parties in the specific ways and circumstances set out in Facebook's privacy policy and with user consent.

195. Facebook materially breached the terms of the Agreement through its unlawful conduct alleged herein, including its disclosure of Plaintiffs' and the Class's sensitive personal information to Cambridge.

196. As a result of Facebook's misconduct and breach of the Agreement described herein, Plaintiffs and the Class suffered damages.

197. Plaintiffs and the Class Members did not receive the benefit of the bargain for which they contracted and for which the paid valuable consideration in the form of their sensitive personal information, which, as alleged above, has ascertainable value to be proven at trial.

198. Plaintiffs and each Class Member gave up something of value, sensitive personal information, in exchange for access to Facebook and Facebook's privacy promises.

199. Facebook materially breached the contracts by violating its privacy terms, thus depriving Plaintiffs and Class members the benefit of the bargain.

200. Thus, their actual and appreciable damages take the form of the value of their sensitive personal information that Facebook wrongfully shared with Cambridge through Facebook's knowledge, neglect or recklessness.

201. The sensitive personal information captured by Facebook and disclosed to Cambridge was an exceptionally egregious breach of trust between Facebook, Plaintiffs

and the Class Members because the sensitive personal information related to voting preferences, political opinions, target news feeds related to potential candidates as well as economic, religious and doctrinal issues that were all related to 2016 Election cycle.

202. Facebook's misconduct was exacerbated by Cambridge efforts to illegally and deceptively influence the 2016 Presidential Election to cause the person who is the current president to be elected.

203. Plaintiffs seek damages based on Facebook's breach of the Agreement, and disgorgement from Facebook of the proceeds that Facebook wrongfully obtained by breaching the Agreement.

204. Plaintiffs also seek damages which are directly resulted from Facebook allowing Cambridge to improperly influence the 2016 Presidential Election, resulting in the election of the current President.

WHEREFORE, Plaintiffs and a nationwide class of Facebook users are entitled to damages, injunctive relief and equitable relief to remedy the above described misconduct.

COUNT V

Tort of Intrusion Upon Seclusion

205. Plaintiffs adopt and incorporate each and every allegation of this complaint as if stated fully herein.

206. Under Illinois common law, a tort of Intrusion Upon Seclusion is committed where a person or entity intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns.

207. Any such person or entity is subject to liability to the other for invasion of his or her privacy if the intrusion would be highly offensive to a reasonable person.

208. Defendants' collective misconduct has led to governmental investigations in England and the United States.

209. Defendants' collective misconduct is outrageous to a reasonable person.

210. Defendants' collective misconduct has led to data breaches and the disclosure of Plaintiffs' personal information by Cambridge and other as yet unknown John and Jane Does.

211. Plaintiffs had a reasonable expectation that their personal information would not be compromised by Defendants Zuckerberg, Facebook, Cambridge and as yet unknown John and Jane Doe Defendants.

212. Defendants' collective misconduct and resultant data disclosures are objectively unreasonable.

213. Accordingly, Defendants Zuckerberg, Facebook, Cambridge and as yet unknown John and Jane Doe Defendants have intruded upon the solitude, seclusion, private affairs and concerns of Plaintiffs and proposed members.

214. Plaintiffs seek damages which are directly resulted from Facebook allowing Cambridge to improperly influence the 2016 Presidential Election, resulting in the election of the current President.

WHEREFORE, Plaintiffs and a nationwide class of Facebook users are entitled to damages, injunctive relief and equitable relief to remedy the above described misconduct.

COUNT VI

Violation of the Illinois Consumer Fraud and Deceptive Practices Act

215. Plaintiffs adopt and incorporate each and every allegation of this complaint as if stated fully herein.

216. As set forth above, Facebook's social media services constitute "conduct of any trade or commerce" as this phrase is defined by and/or used within the Illinois Consumer Fraud and Deceptive Practices Act ("ICFA").

217. Similarly, Cambridge's activities constitute "conduct of any trade or commerce" as this phrase is defined by and/or used within the Illinois Consumer Fraud and Deceptive Practices Act ("ICFA").

218. The ICFA states, in relevant part:

> Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact . . . in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby.

815 ILCS 505/2.

219. "Any person who suffers actual damage as a result of a violation of this Act committed by any other person may bring an action against such person. The court, in its discretion may award actual economic damages or any other relief which the court deems proper." 815 ILCS 505/10a.

220. As set forth above, Defendants Facebook, Cambridge and as yet unknown Does entities violated the ICFA, namely 815 ILCS 505/2, by engaging in unfair, abusive, and deceptive conduct in its transactions with Plaintiffs and other Facebook users.

221. Defendants Facebook, Cambridge and as yet unknown Does entities intended Plaintiffs to rely on their deceptive conduct, statements and communications in order to cause Plaintiffs and other Facebook users to download and utilize the Facebook app and the *MyDigitalLife* app.

222. Defendants Facebook and as yet unknown Does entities obtained compensation in the form of advertising dollars resulting from Plaintiffs' and others' use of the Facebook app.

223. The monies obtained by Defendants Facebook and as yet unknown John and Jane Does and Doe entities through the above alleged misconduct constitute improper income, payment and/or compensation.

224. On information and belief, Defendants Cambridge and as yet unknown John and Jane Does and Doe entities obtained compensation in the form of payment from as yet unknown third parties.

225. The monies obtained by Defendants Cambridge and as yet unknown John and Jane Does and Doe entities through the above alleged misconduct constitute improper income, payment and/or compensation.

226. Plaintiffs have suffered injuries as alleged above.

227. Additionally, Plaintiffs obtained counseling from the undersigned attorney to help them understand and protect their rights under the law.

228. Accordingly, Plaintiffs has been harmed and has suffered damages as a result of Defendant's unlawful collection practices as described herein.

229. Plaintiffs are entitled to relief pursuant to 815 ILCS 505/10a.

WHEREFORE, Plaintiff, individually and on behalf of the other Class members, respectfully requests that this Court enter an Order:

a. Certifying the United States Class and appointing Plaintiffs as Class Representatives;

b. Appointing the undersigned counsel and his firm as Class Counsel;
c. declaring that Defendants' conduct was unlawful, negligent, deceptive, unfair, and unlawful as alleged herein;

d. Enjoining Defendants from further unlawful business practices;

e. Awarding Plaintiffs and the Class Members compensatory and punitive damages;

f. Awarding Plaintiffs and their counsel reasonable attorneys' fees costs and expenses; and

g. Granting such other relief as the Court deems just and proper.

THE ELEMENTS OF A CLASS ACTION ARE SATISFIED

230. Numerosity is satisfied as Defendants Zuckerberg and Facebook have admitted that there are at least 300,000 who were misled and duped by Cambridge, currently unknown John Doe and Jane Doe Defendants, John Doe entities, and unknown third-parties.

231. Joinder of all members of the Class is impracticable.

232. The elements of is commonality and predominance are satisfied.

233. Plaintiffs' and the proposed class members' claims all arise from the same operative facts and are based on the same legal causes of action.

234. In summary, this is a civil action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including: (a) whether Facebook represented that it would safeguard Plaintiffs' and Class members' Personal Information; (b) whether Facebook failed to safeguard Plaintiffs' and Class members' Personal Information; (c) whether Facebook represented that it would safeguard Plaintiffs' and Class members' personal information by preventing third-party apps from misusing Facebook user's personal information; (d) whether Facebook failed to safeguard Plaintiffs' and Class members' personal information by failing to properly vet and/or monitor Cambridge's access to and use of Facebook user data; (e) whether Cambridge improperly obtained access to Plaintiffs' and Class members' personal information without their authorization through Cambridge's misuse of *MyDigitalLife*; (f) whether Cambridge improperly obtained access to Plaintiffs' and Class members'

personal information without their authorization as a result of Cambridge misusing *MyDigitalLife* to gain access to Plaintiffs' and Class members' personal information to the extent to Plaintiffs and Class members did not download *MyDigitalLife* and had their personal information mined as a result of another Facebook "friend" downloading and using the *MyDigitalLife* app., (h) whether Facebook was aware of Cambridge's improper conduct; (i) whether Facebook responded promptly and properly after learning of Cambridge's improper conduct; whether Defendants obtained; and (j) improper income, payment and/or compensation.

235. A class action is an appropriate method for the fair and efficient adjudication of this controversy, and superior to other available methods for the fair and efficient adjudication of this controversy.

236. The common questions of law and fact enumerated above predominate over questions affecting only individual Class members.

237. The likelihood that individual Class members will prosecute separate actions is remote due to the extensive time and considerable expense necessary to conduct such litigation, as well as the absence of a fee shifting mechanism.

238. The expense and burden of individual litigation would make it impracticable for proposed Class members to prosecute their claims individually.

239. Plaintiffs will fairly, adequately and vigorously represent and protect the interests of the proposed class members and have no interests antagonistic to those of the Class. Neither Plaintiff has any defenses unique to them.

240. Plaintiffs' counsel, James C. Vlahakis, is an experienced consumer class action litigator who has defended over a hundred consumer-based claims since 1998. For example, in conjunction with class counsel, Mr. Vlahakis has obtained Court approval of numerous class actions. *See, e.g., In Re Capital One Telephone Consumer*

Protection Act Litigation, 2012-cv-10064 (N.D. Ill.) ($75 million dollar TCPA based automated dialing system settlement); *Prater v. Medicredit, Inc.*, 2014-cv-0159 ($6.3 million dollar TCPA based automated dialing system wrong party settlement); *INSPE Associates v. CSL BIotherapries, Inc.* (N.D. Ill.) ($3.5 million fax based settlement). Vlahakis' co-counsel are competent and experienced consumer rights attorneys.

241. FRCP 23(b)(2) provides that injunctive and declaratory relief are proper where "the party opposing the class has acted or refused to act on grounds that apply generally to the class."

242. Here, the above violations apply generally to the proposed classes.

243. For the above reasons, this Court should declare Defendant's misconduct unlawful and enjoin Defendant from further violating the law.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a jury trial on all claims that are subject to a jury trial.

Plaintiffs VICTOR JAMES COMFORTE, II and
BRENDAN MICHAEL CARR individually
and on behalf of all others similarly situated,

By: /s/James Vlahakis

James Vlahakis (lead counsel)
Joseph Davidson (additional counsel)
SULAIMAN LAW GROUP, LTD.
2500 South Highland Avenue, Suite 200
Lombard, Illinois 60148
(630) 581-5456 telephone
jvlahakis@sulaimanlaw.com
jdavidson@sulaimanlaw.com

[i] *See, HARRY POTTER AND THE DEATHLY HALLOWS*, Chapter 27:

"I haven't got a problem calling him V –" [Harry Potter to Ron Weasley]

"[B]ut the name's been jinxed, Harry, that's how they track people! Using his name breaks protective enchantments, it causes some kind of magical disturbance . . . ."

"Because we used his name?"

"Exactly! You've got to give them credit, it makes sense. It was only people who were serious about standing up to him, like Dumbledore, who ever dared use it. Now they've put a Taboo on it, anyone who says it is trackable – quick and easy way to find Order members!"